WHAT IS CLAIMED IS:

1. A computer-readable medium having computer-executable instructions, comprising:

creating a shadow copy of a volume;

examining the shadow copy to verify an integrity of the volume;

reporting on the integrity of the volume based on the examining of the shadow copy of the volume.

2. The computer-readable medium of claim 1, wherein the volume remains on-line while examining the shadow copy to verify an integrity of the volume.

3. The computer-readable medium of claim 2, wherein the volume is changed while examining the shadow copy to verify an integrity of the volume and wherein verifying the integrity is unaffected by any changes to the volume.

4. The computer-readable medium of claim 1, wherein the volume includes meta-data that comprises entries, wherein at least some of the entries comprise file and directory entries.

5. The computer-readable medium of claim 5, wherein examining the shadow copy to verify an integrity of the volume comprises searching the meta-data for file entries which no directory entry indexes.

6. The computer-readable medium of claim 5, wherein examining the shadow copy to verify an integrity of the volume comprises searching the meta-data for directory entries which index a file entry wherein the file entry does not index the directory entry.

7. The computer-readable medium of claim 5, wherein examining the shadow copy to verify an integrity of the volume comprises searching the meta-data for a directory entry which is indexed by a file entry, wherein the directory entry does not index the file entry.

8. The computer-readable medium of claim 4, wherein at least some of the entries comprise attributes of an object associated with the entry, wherein examining the shadow copy to verify an integrity of the volume comprises examining the at least some of the entries to verify that attributes included in each entry are correct.

9. The computer-readable medium of claim 8, wherein one of the attributes comprises a length of a name of an object associated with the entry including the attribute.

10. The computer-readable medium of claim 4, wherein examining the shadow copy to verify an integrity of the volume comprises searching for unreadable entries in the meta-data.

11. The computer-readable medium of claim 4, wherein the volume includes meta-data that comprises entries and wherein examining the shadow copy to verify an integrity of the volume comprises searching the entries for unreferenced security descriptors.

12. The computer-readable medium of claim 4, wherein the meta-data indicates a hierarchy of the objects contained on the volume.

13. The computer-readable medium of claim 4, wherein the meta-data indicates where objects are stored on the volume.

14. The computer-readable medium of claim 4, wherein the meta-data includes a security descriptor that indicates access rights associated with at least one object on the volume.

15. The computer-readable medium of claim 1 wherein the volume comprises a raw volume.

16. The computer-readable medium of claim 15, wherein the raw volume lacks a table that identifies objects contained on the volume.

17. The computer-readable medium of claim 15, wherein the raw volume includes a disk including partition information.

18. The computer-readable medium of claim 15, wherein the volume is accessed by a database engine.

19. The computer-readable medium of claim 18, wherein examining the shadow copy to verify an integrity of the volume comprises the database engine examining the shadow copy.

20. The computer-readable medium of claim 1, further comprising making the volume available for access while examining the shadow copy to verify the integrity of the volume.

21. The computer-readable medium of claim 1, wherein the shadow copy comprises a logical duplicate of the volume at a selected point in time, wherein the shadow copy maintains data found on the volume at the selected point in time as the volume changes.

22. The computer-readable medium of claim 1, wherein the shadow copy is created via at least one of a copy-on-write and split mirror.

23. A method for verifying an integrity of a volume, comprising:

creating a shadow copy of the volume, the shadow copy comprising a logical duplicate of the volume at a given point in time;

examining the shadow copy to verify an integrity of the volume; and

reporting on the integrity of the volume.

24. The method of claim 23, wherein the shadow copy is created by one of a plurality of shadow copy providers that each exist on a system, each shadow copy provider capable of providing a shadow copy of the volume upon command.

25. The method of claim 23, wherein each shadow copy provider is designed to create a shadow copy for a particular type of application.

26. The method of claim 25, wherein the type of application comprises a volume verification application.

27. The method of claim 23, wherein the volume comprises a volume formatted in accordance with FAT, NTFS, or UDFS.

28. The method of claim 23, wherein the volume comprises a volume formatted for UNIX®, LINUX®, OS/2®, or BeOS®.

29. A system for verifying an integrity of a volume, comprising:

a shadow copy provider arranged to create a shadow copy of a volume;

an API arranged to interface with the shadow copy provider and to instruct the shadow copy provider to create the shadow copy; and

a verify disk component arranged to verify the integrity of the volume by examining the shadow copy of the volume.

30. The system of claim 29, wherein the shadow copy comprises a logical duplicate of the volume at a selected point in time.

31. The system of claim 29, wherein the shadow copy is maintained by actions comprising copying each block that changes on the volume to another location before the block changes, wherein a request to read data from the shadow copy for a block that has changed in the volume is satisfied with data from the other location.

32. A computer-readable medium having computer-executable instructions, comprising:

creating a shadow copy of a disk;

examining the shadow copy to verify an integrity of the disk;

reporting on the integrity of the disk based on the examining of the shadow copy of the disk.